

Rapid7 InsightIDR Customer Case Study: Journal

Introduction

This case study of Journal is based on a March 2022 survey of Rapid7 InsightIDR customers by TechValidate, a 3rd-party research service.



“InsightIDR took us from Zero to Hero and enabled our passing a SOC 2, Type 1 audit the following year.”

Challenges

The business challenges experienced before evaluating and ultimately selecting InsightIDR:

- Difficulty identifying cyber security threats on endpoints
- Lacking SOC efficiency around detection and response
- Dealing with many blind spots across our environment
- Challenged to satisfy compliance and regulatory requirements around log retention and monitoring

Company Profile

Company:
Journal

Company Size:
Small Business

Industry:
Computer Software

Use Case

The key features and functionalities of Rapid7 InsightIDR that the surveyed company uses:

- User Behavior Analytics (UBA)
- Curated Threat Intelligence and Detections
- Endpoint Detection and Response (EDR)
- Cloud Monitoring and Detections
- Centralized Log Management
- Compliance Reporting

They have deployed the Rapid7 Insight Agent across 100% of the assets in their environment. Outcomes realized by leveraging the Insight Agent with InsightIDR:

- Improved endpoint visibility
- Accelerated detection of targeted or compromised assets
- Accelerated time to contain threats on the endpoint

About Rapid7 InsightIDR

Rapid7 is advancing security to accelerate innovation. Learn how our Insight Platform delivers shared visibility, analytics, and automation at www.rapid7.com.

Learn More:

[Rapid7](#)

Results

The surveyed company agreed that Rapid7 InsightIDR helped them to:

- Level up and advance security program
- Spend more time on training and advancing security skills
- Spend more time on innovative work / special projects
- Greatly improve team efficiency
- Reduce team burnout
- Improve work-life balance
- Improve employee retention

Since adopting InsightIDR they stated that they were able to reduce:

- Team time to address an incident by 50% or more
- Mean time to respond (MTTR) by 50% or more
- Mean time to resolution or containment (MTTC) by 50% or more
- Employee downtime as a result of incidents by 50% or more
- Occurrence of false positives by 50% or more